1 4F-1 Bookkeeping

- **0 pts** Correct

Exercise 4F-2. VCGen for Let [6 points]. In class we gave the following rules for the (backward) verification condition generation of assignment and let:

$$\begin{array}{ll} \mathrm{VC}(c_1; c_2, B) & = \mathrm{VC}(c_1, \mathrm{VC}(c_2, B)) \\ \mathrm{VC}(x := e, B) & = [e/x]\ B \\ \mathrm{VC}(\mathsf{let}\ x = e\ \mathsf{in}\ c, B) & = [e/x]\ \mathrm{VC}(c, B) \end{array}$$

That rule for let has a bug. Give a correct rule for let.

$\mathrm{VC}(\mathsf{let}\ x = e\ \mathsf{in}\ c, B) = [x/oldX]([e/x]VC(c, [oldX/x]B))$

Assume $oldX$ is not used in c in: $\mathsf{let}\ x = e\ \mathsf{in}\ c$.

2 4F-2 VCGen for Let

- **0 pts** Correct

Exercise 4F-3. VCGen Mistakes [6 points]. Given $\{A\}c\{B\}$ we desire that $A \implies \text{VC}(c, B) \implies \text{WP}(c, B)$. We say that our VC rules are *sound* if $\models \{\text{VC}(c, B)\}\ c\ \{B\}$. Demonstrate the unsoundness of the buggy let rule by giving the following six things:

1. a command c and
   $c = \{\texttt{let}\ x = 2\ \texttt{in}\ \texttt{y} := \texttt{x} + 2\}$

2. a post-condition B and
   $B = \{x < y\}$

3. a state σ such that
   $\sigma = \{x = 5, y = 4\}$

4. $\sigma \models \text{VC}(c, B)$ and
   $\{x = 1, y = 4\} \models \text{VC}(\texttt{let}\ x = 2\ \texttt{in}\ y := x + 2, B)$

   $\text{VC}(\texttt{let}\ x = 2\ \texttt{in}\ y := x + 2, B) =$
   $[2/x]VC(y := x + 2, B) =$
   $[2/x]([x + 2/y]B) =$
   $[2/x]([x + 2/y]x < y) =$
   $[2/x](x < x + 2) =$
   $(2 < 2 + 2)$

   $\{x = 5, y = 4\} \models (2 < 2 + 2)$

5. $\langle c, \sigma\rangle \Downarrow \sigma'$ but
   $\langle \texttt{let}\ x = 2\ \texttt{in}\ y := x + 2, \{x = 5, y = 4\}\rangle \Downarrow \{x = 5, y = 4\}$
   x is bound to the value 2 in the expression $y := x + 2$, yielding the value of 4 for y in state σ'. However, x is only bound to 2 during the execution of the body of `let`. Thus, in the final evaluated σ' x remains of value 5 as it was not changed from the starting value in σ.

6. $\sigma' \not\models B$.
   $\{x = 5, y = 4\}\rangle \not\models \{x < y\}$

3 4F-3 VCGen Mistakes

- **0 pts** Correct

Exercise 4F-4. Axiomatic Do-While [6 points]. Write a sound and complete Hoare rule for do c while b. This statement has the standard semantics (e.g., c is executed at least once, before b is tested).

$$\frac{\vdash \{A\}\ c\ \{C\} \qquad \vdash \{C\}\ \mathsf{while}\ b\ \mathsf{do}\ c\ \{B\}}{\vdash \{A\}\ \mathsf{do}\ c\ \mathsf{while}\ b\ \{B\}}$$

Submission. Turn in the formal component of the assignment as a single PDF document via the `gradescope` website. Your name and Michigan email address must appear on the first page of your PDF submission but may not appear anywhere else.

4 4F-4 Axiomatic Do-While

- **0 pts** Correct